CLAIMS

What is claimed is:

1. A method for transmitting in encrypted form, from a sender to a receiver, an initially unencrypted message so as to enable, through encryption, verification of authenticity of the sender and of integrity of contents of the message, comprising the steps of:

dividing the unencrypted message to be transmitted into a data section containing the contents of the unencrypted message and a header section;

generating a check element from the contents of the message to be transmitted;

appending the generated check element to the end of the data section;

adding sender identification data to the header section; and

at least one of encrypting and signing of the data section using an encryption method to enable reliable identification of the sender and the receiver of the encrypted message.

2. A method in accordance with claim 1, wherein the check element is generated using a hash function.

3. A method in accordance with claim 1, wherein the encryption method for said at least one of encrypting and signing of the data section comprises a public-private key encryption method.

4. A method in accordance with claim 1, wherein the encryption method for said at least one of encrypting and signing of the data section comprises use of the RSA encryption algorithm.

5. A method in accordance with claim 1, further comprising the step of adding to the header section an identifier of the encryption method used for said at least one of encrypting and signing of the data section.

6. A method in accordance with claim 1, wherein the sender identification data added to the header section comprises identification of an owner of a public key to be used to decrypt and verify a signature of the encrypted message.

7. A method in accordance with claim 1, wherein said step of at least one of encrypting and signing of the data section comprises signing of the data section with a digital signature.

8. A method in accordance with claim 1, wherein said step of at least one of encrypting and signing of the data section comprises signing of the data section using a private key of the sender and the encryption method comprises a public-private key encryption method.

9. A method in accordance with claim 8, wherein said step of at least one of encrypting and signing of the data section further comprises encrypting the signed data section using a public key of the receiver.

10. A method in accordance with claim 9, further comprising the step of decrypting the transmitted encrypted message using a private key of the receiver.

11. A method in accordance with claim 10, further comprising the step of identifying the sender of the transmitted encrypted message by decrypting, after said decrypting of the transmitted encrypted message using the private key of the receiver, the transmitted encrypted message using a public key of the sender.

12. A method in accordance with claim 8, further comprising the step of identifying the sender of the transmitted encrypted message by decrypting the transmitted encrypted message using a public key of the sender.

13. A method in accordance with claim 1, wherein the integrity of the transmitted encrypted message is verified using the check element appended to the data section.

14. A method in accordance with claim 1, further comprising the step of requesting, if errors are detected in the contents of the transmitted encrypted message, retransmission of the encrypted message.

15. A method in accordance with claim 1, further comprising the step of transmitting an acknowledgement of successful transmission of the encrypted message.

16. A method in accordance with claim 1, further comprising the step of transmitting the encrypted message through a mobile communication system.

17. A method in accordance with claim 16, where the mobile communication system comprises a GSM system.

18. A method in accordance with claim 16, wherein said step of at least one of encrypting and signing of the data section being carried out using a mobile station.